

**Midterm 2.** Notes on the questions.

1.  $(12345)(643125) = (56)(132)(4)$  so its order is the least common multiple of 1, 2, and 3, which is 6. The permutation is the product of a 2 cycle (odd) and a 3-cycle (even) so it is an odd permutation.
2. If  $a$  and  $b$  are real then  $N(a + bi) = a^2 + b^2$ .  $N(xy) = xy\bar{xy} = x\bar{x}y\bar{y} = N(x)N(y)$ . We have

$$\begin{aligned}(a^2 + b^2)(c^2 + d^2) &= N(a + bi)N(c + di) \\ &= N((a + bi)(c + di)) \\ &= N(ac - bd + i(ad + bc)) \\ &= (ac - bd)^2 + (ad + bc)^2\end{aligned}$$

- Note that  $13 = 3^2 + 2^2$  and  $101 = 10^2 + 1^2$ . So by the formula above  $1313 = (3 \times 10 - 2 \times 1)^2 + (3 \times 1 + 2 \times 10)^2 = 28^2 + 23^2$ . Another solution is  $1313 = (2 \times 10 - 3 \times 1)^2 + (2 \times 1 + 3 \times 10)^2 = 17^2 + 32^2$ .
3. First find an irreducible polynomial over the field with 13 elements.  $x^2 - a$  will do for any  $a$  that is not a square; for example, we could choose  $a = 2$  and take the polynomial to be  $p(x) = x^2 - 2$ . Then  $F_{13}[x]/(p(x))$  is a field with  $13^2$  elements. (Note that  $x^2 + 1$  does NOT work as it is reducible over  $F_{13}$ .)
  4.
    - (a) Any polynomial of odd degree over the reals has a root (as it has different signs for  $x$  large and positive and for  $x$  large and negative). So any polynomial of odd degree at least 3 over the reals is reducible.
    - (b) The polynomial has degree at most 3, so it is irreducible if and only if it has no roots over  $F_2$ . There are only 2 elements 0 and 1 of  $F_2$  to check as roots. As  $f(0)$  and  $f(1)$  are both nonzero the polynomial  $f(x) = x^3 + x + 1$  is irreducible.
    - (c) This polynomial is reducible, as it is equal to  $(x^2 + x + 1)^2$ . To test this polynomial, first check it has no roots, the check for divisibility by polynomials of degree 2. This is not too hard as  $x^2 + x + 1$  is the only irreducible polynomial of degree 2 over  $F_2$ . (There is also a fast way to see it is reducible that one or two people used: recall that  $a^2 + b^2 + c^2 + \dots = (a + b + c + \dots)^2$  whenever  $2 = 0$ . So any sum of squares in a ring where  $2=0$  is also a square. But  $x^4 + x^2 + 1 = (x^2)^2 + (x)^2 + 1^2$  is obviously a sum of squares.)
  5. Use Euclid's algorithm:

$$\begin{aligned}x^5 + 1 &= (x^2 + 1)(x^3 + x) + (x + 1) \\ x^2 + 1 &= (x + 1)(x + 1) + 0\end{aligned}$$

So the greatest common divisor is  $x + 1$ . The first line gives  $x + 1 = (x^3 + x)(x^2 + 1) + 1 \times (x^5 + 1)$  so we can put  $a(x) = x^3 + x$ ,  $b(x) = 1$ . Several people worked over the rationals rather than over  $F_2$ . In this case the greatest common divisor is 2 (or 1),  $a(x) = x^4 - x^3 - x^2 + x + 1$  and  $b(x) = 1 - x$ .